A

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/634,117	08/04/2003	James M. Doherty	1033-T00534	5753

60533 7590 07/20/2006

TOLER SCHAFFER, LLP
5000 PLAZA ON THE LAKES
SUITE 265
AUSTIN, TX 78746

EXAMINER
HOANG, DANIEL L

ART UNIT	PAPER NUMBER
2192	

DATE MAILED: 07/20/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	**Application No.** 10/634,117	**Applicant(s)** DOHERTY ET AL.
	Examiner Daniel L. Hoang	**Art Unit** 2192

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *11/4/2003; 1/3/2003*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-27* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-27* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *8/04/03* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date *11/04/03; 1/03/06*.
4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

Claim Rejections - 35 USC § 112

The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

1. Claims 2, 14, and 16 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which are not described in the specification in such a way as to enable one skilled in the art to which it pertains, or with which it is most nearly connected, to make and/or use the invention. More specifically, JTRIP is not adequately described. For purposes of examination, examiner will interprets a "JTRIP system daemon" as a program capable of intrusion detection.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

2. Claims 1-27 rejected under 35 U.S.C. 103(a) as being unpatentable over Douglas (US PGP 20040049693) and further in view of Mann (US Patent No. 6,081,894).

With respect to claim 1, Douglas teaches:

A method comprising:

providing a host computer system having at least one network interface interfaced with a computer network; **(see figure 1A)**

operating the host computer system in a multi-user mode; **(see figure 1A)** detecting an intrusion event using a system daemon; **(see figure 2, element 22).**

Douglas does not expressly disclose responding to the detection of the intrusion event by isolating at least one network interface from the computer network and limiting physical access to the host computer system by taking the host computer down to a single user state.

Mann teaches:

In response to detecting the intrusion event, isolating at least one network interface from the computer network and taking the host computer system down to a single user state so that access to the host computer system is limited to physical access at the host computer system **(column 3, lines 2-5).**

It would have been obvious at the time that the invention was made to a person of ordinary skill in the art to which the subject matter pertains to modify Douglas' invention so that when an intrusion is detected on the host system, the host can be isolated from the remote devices in order to prevent propagation of the intrusion.

With respect to claim 2, Douglas teaches:

A JTRIP system daemon. **(see figure 2, Administration Engine, AE)**

With respect to claims 3 and 4, the Douglas reference discloses his invention's capability of being implemented on UNIX platforms. The Douglas reference does not expressly disclose isolating the network by issuing an IFCONFIG down command or taking down the host computer system by issuing an INIT1 command. It was well recognized to those of ordinary skill in the pertinent arts that IFCONFIG and INIT1 are UNIX commands used to shut down network interfaces and taking machines offline, respectively. Because the Douglas reference discloses UNIX, it would have been obvious to one of ordinary skill in the art to use the built-in IFCONFIG and INIT1 functions to shut down network interfaces and take machines offline.

With respect to claim 5, Douglas teaches:

Reading, by the system daemon, a configuration file that indicates at least one file in a file system of the host computer system to be monitored for intrusion. **(see figure 2, elements 22 and 22b)**

With respect to claim 6, Douglas teaches:

A directive type that indicates a file to be monitored for intrusion, **(see paragraph 57, module 22b)**

A directive type that indicates a directory whose members are to be monitored for intrusion, **(see figure 13A, "/etc/passwd", system is capable of scanning user directories),** and

A directive type that indicates another configuration file to be monitored for intrusion **(see figure 11A-11C, myfconfigfile.cfg, dragon.cfg)**.

With respect to claim 7 and 8, Douglas teaches:

Computing a data verification signature for a monitored file in a file system of the host computer system', and comparing the data verification signature to a valid data verification signature for the monitored file; wherein said detecting the intrusion event comprises detecting that the data verification signature differs from the valid data verification signature. **(see paragraphs 105 and 106)**

Douglas also teaches the above wherein the valid data verification signature comprises a Message Digest 5 (MD5) signature. **(see paragraphs 105 and 106)**

With respect to claim 9, Douglas teaches:

Reading the valid data verification signature for the monitored file from a database that is located on a second computer system isolated physically and programmatically from the host computer system. **(see paragraph 56, lines 10-18)**

With respect to claim 10, Douglas teaches:

Writing a log of the intrusion event to a log database that is not located on the host computer system or second computer system. **(see paragraph 40)**

With respect to claim 11, Douglas teaches:

Detecting an incorrect permission associated with a file in a file system of the host computer system. **(see paragraph 94)**

With respect to claim 12, Douglas teaches:

Detecting an incorrect ownership associated with a file in a tile system of the host computer system. **(see paragraphs.97 and 98)**

With respect to claim 13, Douglas teaches:

Detecting that a file no longer exists in a file system of the host computer system. **(see paragraph 96)**

Claim 14 is rejected by Douglas and Mann as applied to claims 1-8 and 10.

Claim 15 is rejected by Douglas and Mann as applied to claim 1.

Claim 16 is rejected by Douglas and Mann as applied to claim 2.

Claim 17 is rejected by Douglas and Mann as applied to claim 3.

Claim 18 is rejected by Douglas and Mann as applied to claim 4.

Claim 19 is rejected by Douglas and Mann as applied to claim 5.

Claim 20 is rejected by Douglas and Mann as applied to claim 6.

Claim 21 is rejected by Douglas and Mann as applied to claim 7.

Claim 22 is rejected by Douglas and Mann as applied to claim 8.

Claim 23 is rejected by Douglas and Mann as applied to claim 9.

Claim 24 is rejected by Douglas and Mann as applied to claim 10.

Claim 25 is rejected by Douglas and Mann as applied to claim 11.

Claim 26 is rejected by Douglas and Mann as applied to claim 12.

Claim 27 is rejected by Douglas and Mann as applied to claim 13.

The following patents are cited to further show the state of the art with respect to intrusion detection systems.

US Patent No. 7,032,114 to Moran, which is cited to show an intrusion detection system.

US Patent No. 6,647,400 to Moran, which is cited to show an intrusion detection system that logs communication within a log file.

US PGP 2001/0025311 to Arai et al., which is cited tó show file authorization and access control.

US PGP 2002/0046275 to Crosbie et al., which is cited to show a system for network based intrusion detection and response.

US PGP 2002/0083343 to Crosbie et al., which is cited to show a host based intrusion detection system.

US PGP 2003/0126468 to Markham, which is cited to show a network wherein if a host is compromised, said host is isolated from the network.

Kim, Gene H. and Spafford, Eugene H. "The Design and Implementation of Tripwire: A File System Integrity Checker" February 28, 1995

Lindquidst, Ulf and Porras, Phillip A. "eXpert-BSM: A Host-based Intrusion Detection Solution for Sun Solaris" December 10, 2001

*. Any response to this Office Action should be **faxed to** (571) 273-8300 **or mailed to**:

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Hand-delivered responses should be brought to

Customer Service Window
Randolph Building
401 Dulany Street
Alexandria, VA 22314

*. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Daniel L. Hoang whose telephone number is 571-270-1019. The examiner can normally be reached on Monday - Thursday, 8:00 a.m. - 5:00 p.m., EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, David Robertson can be reached on 571-272-4186. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Daniel L. Hoang
DLH/dlh

DAVID ROBERTSON
SUPERVISORY PATENT EXAMINER